IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICHAEL BRIGGS, on behalf of himself and all others similarly situated,

Plaintiff,

v.

THE NORTH HIGHLAND COMPANY,

Defendant.

Case No. 1:22-cv-03640

First Amended Complaint – Class Action

Demand for Jury Trial Enclosed

INTRODUCTION

1. This case arises from a data breach. *See* Notice of Data Breach (Exhibit 1). Defendant The North Highland Company is a sophisticated consultancy firm. It collects and stores vast amounts of highly sensitive data about its employees—including their background checks, performance evaluations, medical information, bank account numbers, and social security numbers. North Highland's employees have no choice but to provide North Highland with their information in and trust North Highland to keep their data secure.

2. Ironically, North Highland touts its "cybersecurity expertise," going so far as to publish a white paper with its "insights" for prospective clients. *See Cybersecurity Help Wanted* at 2, 12 (2018) (Exhibit 2). It did not put those insights to use in this case.

3. In a story that has become all too familiar, an unauthorized third-party executed a successful ransomware attack on North Highland's system and absconded with employees' personally identifying information (PII). Criminals can now sell the victims' data on the black market for the purpose of stealing their identities. None of this would have occurred if North Highland had implemented reasonable data security measures—measures that North Highland itself has identified as reasonable to its clients.

4. Plaintiff Michael Briggs was a victim of the data breach. He brings this action on behalf of himself and all others similarly situated, seeking damages for the injuries that North Highland's negligence and will cause, as well as injunctive relief to ensure that the data North Highland continue to store will be protected by reasonable data security practices going forward.

PARTIES

5. Plaintiff Michael Briggs is a resident of Tallahassee, Florida. He was employed by North Highland as an associate Vice President from October 2018 until September 2019.

6. Defendant The North Highland Company is a corporation with a principal place of business in Atlanta, Georgia.

7. On information and belief, North Highland made the decisions giving rise to the data breach from its Georgia headquarters—including decisions regarding its data security policy and procedures, as well as its response to the May 26, 2022 data breach.

JURISDICTION AND VENUE

8. The Court has personal jurisdiction over North Highland because North Highland's principal place of business is located in Atlanta, Georgia.

9. This Court has subject-matter jurisdiction under 28 U.S.C. § 1332(d)(2) because at least one member of the proposed Class, including Briggs, is a citizen of a state different from that of North Highland; the amount in controversy exceeds $5,000,000, exclusive of interest and costs; the proposed Class consists of more than 100 class members, and none of the exceptions under the subsection apply to this action.

10. Venue is proper because North Highland's principal place of business is located in the Northern District of Georgia. *See* 28 U.S.C. § 1391(b)(1).

FACTUAL ALLEGATIONS

A. North Highland allowed Briggs's data to be stolen.

11. According to the data breach notice that North Highland sent to Briggs, a hacker gained access to North Highland's system on or around May 26, 2022. A true and correct copy of the Notice Letter is attached as Exhibit 1

12. The hacker executed a ransomware attack, which North Highland discovered on June 6, 2022.

13. North Highland confirmed on June 28, 2022 that the hackers exfiltrated files containing personal information of current and former North Highland employees.

14. The information that the hackers exfiltrated includes: names, national insurance numbers, social security numbers, tax numbers, addresses, bank account numbers and other payroll information, personal phone and email addresses, dates of birth, benefits information, background check and employment screening information, performance related records, health-related information, and other employment-related information.

15. Since discovering the data breach, North Highland has "initiated a number of technical remediation efforts, including new password requirements for all employees." Exhibit 1. On information and belief, those remediation efforts would have prevented the breach in the first place, and any reasonable person would have known to implement them.

16. "To help protect [class members'] identity," North Highland offered Plaintiff and class members two-years of identity monitoring for the "detection and resolution of identity theft." Exhibit 1. This service includes monitoring for fraud, identity restoration, and up to $1 million of identity theft insurance. Therefore, North Highland itself understands that: (1) Plaintiff and class members are at a substantial risk of identity theft; (2) the risk will continue for multiple years; and (3) identity theft can cause at least $1 million in damages.

17. North Highland also provided Plaintiff and class members with instructions on reviewing their accounts for signs of fraud or identity theft, placing fraud alerts on their credit reports, and reporting identity theft to the

police or FTC. This further demonstrates North Highland's knowledge of the substantial risk of identity theft faced by Plaintiff and class members.

B. The data breach was highly foreseeable, yet North Highland failed to take reasonable precautions.

18. Given the type of data that North Highland collected and stored, it was highly foreseeable that bad actors would attempt to access it without permission.

19. "[H]ackers are likely to be drawn to databases containing information which has a high value on secondary black markets," such as "identifying and financial data." Mark Verstraete & Tal Zarsky, *Optimizing Breach Notification*, 2021 U. ILL. L. REV. 803, 854–55 (2021). Consequently, "relevant and rational firms should engage in greater security investment and reduced collection—all steps to limit the prospects of a potential breach and subsequent notification." *Id.* at 855.

20. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

21. Because North Highland collected and stored identifying and financial information that is very valuable to criminals, it was highly foreseeable that a bad actor would attempt to access that data without permission.

22. North Highland frequently collects and stores personally identifying and financial information. Therefore, the burden (if any) of implementing reasonable data security practices is minimal in comparison to the substantial and highly foreseeable risk of harm.

23. North Highland has known about these substantial risks for many years prior to the data breach. In a 2018 white paper, North Highland emphasized its "cybersecurity expertise" and stressed the importance of data security in the wake of the Equifax data breach, given that "cyber criminals are working to score a bigger payday" and "[e]xperts agree that it is only matter of time before a new company takes Equifax's place in the spotlight." *Cybersecurity Help Wanted* at 3, 12.

24. North Highland is aware that "cybersecurity threats are evolving fast." *Id.* at 4. As companies have digitize more of their operations, "the scope, scale, and impact of cybersecurity risks grow in concert with rapidly evolving technologies." *Id.* For example, "[t]he expanding universe of Internet of Things (IoT) devices is particularly vulnerable to exploitation as companies may not update them after installation, and many devices are not able to receive security update patches." *Id.* The Internet of Things is a common vector for ransomware attacks and, on information and belief, North Highland failed to take reasonable care to avoid its own IoT devices being used to perpetrate the ransomware attack.

25. North Highland is also aware that companies must "make above-average investments of time and money" to combat evolving cybersecurity

risks. *Id.* at 5. On information and belief, North Highland failed to make reasonable, much less "above-average," investments of time in money to protect its own employees' data.

26. North Highland is aware that "burnout" among cybersecurity teams "directly contributes to increased risk" of a data breach. *Id.* at 6. On information and belief, North Highland's employees were overworked to the point of burnout, which directly caused errors leading to the data breach

27. North Highland is aware that "84 percent of data breaches are at least in part attributable to human error." *Id.* Yet, on information and belief, North Highland failed to adequately train its employees on even the basic cybersecurity protocols, including:

a. Effective password management and encryption protocols, including, but not limited to, the use of multi-factor authentication for all users;
b. Locking, encrypting and limiting access to computers and files containing sensitive information;
c. Implementing guidelines for maintaining and communicating sensitive data;
d. Protecting sensitive employee information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients; and
e. Providing focused cybersecurity awareness training programs for employees.

28. According to North Highland, there are three "fundamentals of a cybersecurity workforce strategy:" (1) "know your landscape," (2) "identify the precise skills and talents you need," and (3) "establish targeted employee

development programs." *Id.* at 9. On information and belief, North Highland failed to adhere to those fundamentals when formulating its own cybersecurity workforce strategy, which resulted in the data breach.

29. North Highland is aware that cybersecurity teams should include an adequate number of individuals experienced in the relevant "security disciplines," including "Identity and Access Management (IAM, Incident Response, Regulation and Compliance." *Id.* at 10. On information and belief, North Highland's cybersecurity workforce was not comprised of individuals with the relevant security disciplines, which resulted in the data breach.

30. North Highland has extensive "cybersecurity expertise." *Id.* at 12. Its failure to use its expertise in this case was unreasonable under the circumstances and caused the data breach.

31. Moreover, North Highland has provided cybersecurity consultations to many companies. On information and belief, North Highland recommended many reasonable practices and procedures that it did not itself adhere to.

32. In addition, the FTC has noted the need to factor data security into all business decision-making. *Start With Security, A Guide for Business*, FTC (accessed June 9, 2022), https://bit.ly/3mHCGYz. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested

and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software. *Id.*

33. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These

orders, which all preceded the data breach, further clarify the measures businesses must take to meet their data security obligations.

34. On information and belief, Defendant's use of outdated and insecure computer systems and software that are easy to hack, and their failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

35. Defendant violated its obligation to implement best practices and comply with industry standards concerning computer system security, which allowed class members' data to be accessed and stolen by criminals.

C. Briggs's information was exposed in the data breach, which caused him to suffer concrete injuries.

36. Plaintiff Michael Briggs was an employee of North Highland for about eleven months. He entrusted North Highland with his personally identifying and financial information as a condition of his employment.

37. Briggs received a data breach notification informing him that his personally identifying and financial information was accessed in the breach. Criminals now have extensive, personally identifying data concerning Briggs, including his: name, national insurance numbers, social security numbers, tax numbers, addresses, bank account numbers and other payroll information, personal phone and email addresses, dates of birth, benefits information, background check and employment screening information,

performance related records, health-related information, and other employment-related information. *See* Exhibit 1.

38. Briggs typically takes measures to protect his PII and is very careful about sharing his PII. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

39. As a result of the data breach, Briggs suffered a severe privacy injury. Briggs, like any reasonable person, strongly prefers to keep private his medical information, background checks, performance reviews, and other highly personal information. Because a criminal obtained access to that information, any person can now purchase highly sensitive information about Briggs on the black market. North Highland's negligence thus caused Briggs and the Class to suffer a legally cognizable privacy injury.

40. North Highland is well-aware that individuals expect companies to keep their sensitive information private. It acknowledged that "[t]he damage of a data breach goes well beyond the immediate bottom-line impact of settlements and clean-up. Customer trust is often inexorably damaged, with a whopping 70 percent of consumers reporting that they would stop doing business with an organization if it experienced a data breach." *Cybersecurity Help Wanted* at 4–5. Much like consumers, employees must trust their employers to keep their data secure. A violation of that reasonable expectation of privacy is an actual, concrete injury.

41. Plaintiff also suffered a loss of time, as he has spent and continues to spend a considerable amount of time on issues related to this

Data Breach. In response to the data breach, Plaintiff has spent significant time monitoring his accounts and credit score. This is time that was lost and unproductive and took away from other activities and duties.

42. Plaintiff also suffered actual injury in the form of damages to, and diminution in, the value of his PII—a form of intangible property that he entrusted to Defendant—which was compromised in and as a result of the data breach.

43. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the data breach and has anxiety and increased concerns for the loss of his privacy.

44. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of criminals.

45. Defendant continue to maintain Plaintiff's and class members' PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

46. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the data breach. As a result of the data breach,

Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

47. Because their personally identifying and financial information has been accessed by criminals, Plaintiff and the Class have suffered concrete and ongoing injuries.

48. Plaintiff and the Class are at an imminent and substantial risk of identity theft.

49. According to experts, one out of four data breach notification recipients become a victim of identity fraud. *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, THREATPOST.COM (Feb. 21, 2013), https://bit.ly/3zB8Uwv.

50. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PHI can be worth up to $1,000.00 depending on the type of information obtained. *See* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web*, EXPERIAN (Dec. 15, 2017), https://bit.ly/2Ox2SGY.

51. The value of Plaintiff's and the proposed Class PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

52. It can take victims years to spot identity or PII theft, giving criminals plenty of time to milk that information for cash.

53. One such example of criminals using PII for profit is the development of "Fullz" packages. "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY (Sep. 18, 2014), https://bit.ly/3Qj2eJd.

54. Cyber-criminals can cross-reference two sources of PII to marry unregulated or partial data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete "Fullz" dossiers on individuals.

55. The development of "Fullz" packages means that stolen PHI from the data breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI stolen by the cyber-criminals in the data breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is likely what is already happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the data breach.

56. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

57. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."

58. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

59. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

60. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class will need to be remain vigilant against unauthorized data use for years or even decades to come.

61. Moreover, the breach has diminished the value of Plaintiff and the Class's personal information.

62. The FTC has recognized that consumer data is a new and valuable form of currency. In a FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency." *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FTC (Dec. 7, 2009), https://bit.ly/3xKfzmu.

63. Since it was included in the breach, Plaintiff and the Class's information has already been accessed by criminals, which decreases its value in the marketplace.

64. Therefore, the value of Plaintiff and the Class's personal information was reduced by the data breach.

65. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

66. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

67. None of those injuries would have occurred if Defendant had implemented reasonable data security practices.

CLASS ACTION ALLEGATIONS

68. Pursuant to FED. R. CIV. P. 23(b)(2) and (b)(3), Plaintiff seeks certification of a Class defined as follows:

> All current and former North Highland employees whose personal information was compromised in

> connection with the data breach affecting North Highland Company on or around May 26, 2022, including all those who received notice of the breach.

69. Excluded from the Class are: (a) Defendant and its officers, directors, legal representatives, successors and wholly or partly owned subsidiaries or affiliated companies; (b) class counsel and their employees; and (c) the judicial officers and their immediate family members and associated court staff assigned to this case.

70. *Ascertainability*. The Class can be readily identified through North Highland's records, which is demonstrated by the fact that many class members have already been identified and sent notice letters regarding the data breach.

71. *Numerosity*. North Highland is a major consultancy firm with more than a dozen offices in the United States. On information and belief, North Highland has thousands of current and former employees whose personal information was exposed in the data breach. Therefore, the Class is so numerous that individual joinder is impracticable.

72. *Typicality*. Plaintiff's claims are typical of the Class he seeks to represent. Like all class members, Plaintiff's personal information was exposed in the data breach as a result of Defendant's failure to implement reasonable data security measures. Thus, Plaintiff's claims arise out of the same conduct and are based on the same legal theories as those of the absent class members.

73. *Adequacy of Class Representative.* Plaintiff will fairly and adequately protect the interests of the Class. He is aware of his fiduciary duties to absent class members and is determined to faithfully discharge his responsibility. Plaintiff's interests are aligned with (and not antagonistic to) the interests of the Class.

74. *Adequacy of Counsel.* In addition, Plaintiff has retained competent counsel with considerable experience in class action and other complex litigation, including data breach cases. Plaintiff's counsel have done substantial work in identifying and investigating potential claims in this action, have considerable knowledge of the applicable law, and will devote the time and financial resources necessary to vigorously prosecute this action. They do not have any interests adverse to the Class.

75. *Commonality and Predominance.* This case presents numerous questions of law and fact with answers common to the Class that predominate over questions affecting only individual class members. Those common questions include:

a. Whether Defendant had a duty to use reasonable care to safeguard Plaintiff and the Class's PII;

b. Whether Defendant breached the duty to use reasonable care to safeguard the Class's PII;

c. Whether Defendant breached its contractual promises to safeguard Plaintiff and the Class's PII;

d. Whether Defendant knew or should have known about the inadequacies of their data security policies and system and the dangers associated with storing sensitive PII;

e. Whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect

Plaintiff and the Class's PII from unauthorized release and disclosure;

f. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiff and the Class's PII from unauthorized release and disclosure;

g. Whether the data breach was caused by Defendant's inadequate cybersecurity measures, policies, procedures, and protocols;

h. Whether Defendant is liable for negligence, gross negligence, or recklessness;

i. Whether Defendant's conduct, practices, statements, and representations about the data breach of the PII violated applicable state laws;

j. Whether Plaintiff and the Class were injured as a proximate cause or result of the data breach;

k. What the proper measure of damages is; and

l. Whether Plaintiff and the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

76. *Superiority and Manageability*. A class action is superior to individual adjudications because joinder of all class members is impracticable, would create a risk of inconsistent or varying adjudications, and would impose an enormous burden on the judicial system. The amount-in-controversy for each individual class member is likely relatively small, which reinforces the superiority of representative litigation. As such, a class action presents far fewer management difficulties than individual adjudications, preserves the resources of the parties and the judiciary, and protects the rights of each class member.

77. *Injunctive or Declaratory Relief.* In addition, Defendant acted or failed to act on grounds that apply generally to the Class, such that final injunctive or declaratory relief as to any one class member is appropriate as to all class members.

CAUSES OF ACTION

Count 1: Negligence

On Behalf of Plaintiff and the Class

78. Plaintiff incorporates paragraphs 1–77 by reference.

79. North Highland owed a duty to reasonably safeguard data that Plaintiff and the Class entrusted to it in the scope of their employment. *See Ramirez v. Paradies Shops, LLC*, ___ F.4th ___, 2023 U.S. App. LEXIS 13899, *11 (11th Cir. June 5, 2023).

80. Indeed, North Highland has a special relationship (employer-employee) with Plaintiff and the Class that obligated it to protect them from reasonably foreseeable harms.

81. It was highly foreseeable that a failure to reasonably safeguard Plaintiff and the Class's PII would lead to a data breach. Plaintiff and the Class are members of a well-defined, foreseeable, and probable group of individuals whom North Highland knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff and the Class's personal and financial information in the conduct of its business, and Defendant retained that information.

82. As set forth above, North Highland breached its duty of reasonable care on many levels, including but not limited to, its failure:

a. To use its heightened cybersecurity expertise to avoid causing the data breach, including by adhering to the recommendations in its cybersecurity white papers;

b. To implement industry-standard security procedures sufficient to reasonably protect the information from the data breach;

c. To implement industry-standard security procedures for detecting and responding to an actual or attempted data breach;

d. To reasonably train its employees on data security procedures; and

e. To reasonably supervise its agents, contractors, vendors, and suppliers who were charged with handling and securing the PII of Plaintiff and the Class.

83. North Highland's breach of its duty of care was willful or reckless. North Highland was well aware of the cybersecurity risks that result from unreasonable data security practices, yet it consciously disregarded those risks without adequate justification.

84. North Highland's recklessness or negligence directly and foreseeably caused Plaintiff and the Class's injuries, including, without limitation, theft of their PII by criminals, loss of privacy, improper disclosure of their PII, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach. But-for North Highland's recklessness or negligence, those injuries would not have occurred.

Count 2: Negligence Per Se

On Behalf of Plaintiff and the Class

85. Plaintiff incorporates paragraphs 1–77 by reference.

86. Pursuant to the FTC Act, 15 U.S.C. § 45, North Highland had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

87. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class's sensitive PII.

88. North Highland violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' PII and not complying with applicable industry standards as described in detail herein. North Highland's conduct was particularly unreasonable given the nature and amount of PII that North Highland had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its employees in the event of a breach, which ultimately came to pass.

89. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous

enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

90. North Highland had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII.

91. North Highland breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

92. North Highland's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

93. As a direct and proximate result, Plaintiff suffered actual losses and damages, including, without limitation, theft of his PII by criminals, loss of privacy, improper disclosure of his PII, lost value of his PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by North Highland's negligence. But-for North Highland's negligence, those injuries would not have occurred.

Count 3: Breach of Contract

On Behalf of Plaintiff and the Class

(In the Alternative to Counts 1 and 2)

94. Plaintiff incorporates paragraphs 1–77 by reference.

95. Plaintiff and the Class entered employment contracts with North Highland, in which they provided services in exchange for consideration.

96. As a condition of those contracts, North Highland required Plaintiff and the Class to provide it with their PII.

97. Implicit in this agreement was the understanding that North Highland would exercise reasonable care to safeguard Plaintiff and the Class's PII.

98. North Highland knew that its employees reasonably expected that it would take reasonable precautions to safeguard the PII they provided in the course of their employment.

99. North Highland failed to reasonably safeguard Plaintiff and the Class's PII in many respects, including, but not limited to, its failure:

a. To use its heightened cybersecurity expertise to avoid causing the data breach, including by adhering to the recommendations in its cybersecurity white papers;
b. To implement industry-standard security procedures sufficient to reasonably protect the information from the data breach;
c. To implement industry-standard security procedures for detecting and responding to an actual or attempted data breach;
d. To reasonably train its employees on data security procedures; and
e. To reasonably supervise its agents, contractors, vendors, and suppliers who were charged with handling and securing the PII of Plaintiff and the Class.

100. If Plaintiff and the Class had known that North Highland would not implement reasonable safeguards to protect their PII, they would not have accepted employment the rates that they did. To the contrary, they would have demanded higher wages to the account for the increased risk of harm. By failing to exercise reasonable care, North Highland therefore deprived Plaintiff and the Class of the benefit of the bargain.

101. As a direct and proximate result of North Highland's breach of contract, Plaintiff suffered actual losses and damages, including, without limitation, theft of his PII by criminals, loss of privacy, improper disclosure of his PII, lost value of his PII, and lost time and money incurred to mitigate and remediate the effects of the data breach.

PRAYER FOR RELIEF

102. Plaintiff, individually and on behalf of all others similarly situated, hereby demands:

a. Certification of the proposed Class;
b. Appointment of the undersigned counsel as class counsel;
c. An award of all damages, including attorneys' fees and reimbursement of litigation expenses, recoverable under applicable law;
d. Restitution or disgorgement of all ill-gotten gains; and
e. Such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

103. Plaintiff demands a jury trial on all applicable claims.

Respectfully submitted,

By: /s/ *Jared W. Connors*

MEYER WILSON CO., LPA
Matthew R. Wilson (871480)
Email: mwilson@meyerwilson.com
Michael J. Boyle, Jr. (*pro hac vice*)
Email: mboyle@meyerwilson.com
Jared W. Connors (*pro hac vice*)
Email: jconnors@meyerwilson.com
305 W. Nationwide Blvd.
Columbus, Ohio 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066

TURKE & STRAUSS LLP
Samuel J. Strauss (*pro hac vice*)
sam@turkestrauss.com
Raina Borrelli (*pro hac vice*)
raina@turkestrauss.com
613 Williamson St., #201
Madison, WI 53703
P: (608) 237-1775

Counsel for Plaintiff and the Proposed Class